REMARKS

The Office Action dated October 24, 2005 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto. Claims 7-9 and 11-33 are respectfully submitted for consideration.

Claims 8, 9, 11-20, 27-29 and 31-33 were rejected under 35 USC § 103(a) as being unpatentable over U.S. Patent No. 6,400,707 (Baum) in view of U.S. Patent No. 6,233,234 (Curry) and U.S. Patent No. 6,085,328 (Klein). According to the Office Action, Baum substantially teaches the limitations of the claims except for assigning priority to the packets and storing the generated filter in a filter table as recited in claims 8, 9, 11-20, 27-29 and 31-33. Thus, the Office Action combines the teachings of Curry and Klein with the teachings of Baum to yield all of the elements of claims 8, 9, 11-20, 27-29 and 31-33. The rejection is traversed as being based on references that neither teach nor suggest the novel combination of features clearly recited in independent claims 11, 15, 20, 31 and 32.

Claim 11, upon which claims 7-9 and 12-14 are dependent, recites a method for switching VOIP packets in a data network. The method includes the steps of receiving a first packet in a network switch and determining if the first packet is a VOIP packet. The method also includes the step of determining a dynamically negotiated VOIP port for a VOIP session from at least one of the first packet and a second packet received in the network switch, if the first packet is determined to be the VOIP packet. The method

further includes the step of classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters and associating a priority with the subsequent packets to avoid network congestion. The step of classifying all subsequent VOIP packets further includes storing the dynamically negotiated VOIP port, filtering all packets coming through the network switch having the dynamically negotiated VOIP port associated therewith and classifying filtered packets in accordance with predefined filtering actions. The step of storing the dynamically negotiated VOIP port further includes generating a filter corresponding to the dynamically negotiated VOIP port and storing the generated filter in a filter table associated with a fast filtering processor.

Claim 15, upon which claims 16-19 depend, recites a method for switching VOIP packets. The method includes the steps of filtering packets received in a network switch to trap at least one VOIP call setup message and determining a dynamically negotiated VOIP port. The method also includes the steps of filtering all subsequent packets associated with the dynamically negotiated VOIP port and taking predefined filtering actions upon the subsequent packets. The method further includes the steps of classifying all subsequent packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters and associating a priority with the subsequent packets to avoid network congestion. The method also includes the step of taking predefined filtering actions upon the subsequent packets. The steps of filtering packets and determining the dynamically negotiated VOIP port further includes generating a filter

corresponding to the dynamically negotiated VOIP port and storing the generated filter in a filter table associated with a fast filtering processor.

Claim 20, upon which claims 21-30 are dependent, recites a network switch for switching VOIP packets. The network switch includes at least one data port interface controller supporting a plurality of data ports for transmitting and receiving data and a fast filtering processor in communication with the at least one data port interface. The network switch also includes at least one filtering table in communication with the fast filtering processor. The fast filtering processor is configured to snoop packets being transmitted through the network switch to trap a VOIP call setup message, and thereafter, determine a dynamically negotiated VOIP port so that all subsequent VOIP packets can be filtered and assigned an appropriate priority.

Claim 31 recites a method for switching VOIP packets in a data network. The method includes the steps of receiving a first packet in a network switch, determining if the first packet is a VOIP packet, determining a dynamically negotiated VOIP port for a VOIP session from at least one of the first packet and a second packet received in the network switch, if the first packet is determined to be the VOIP packet. The method also includes the steps of classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters and associating a priority with the subsequent packets to avoid network congestion. The steps of determining if the first packet is a VOIP packet, determining a dynamically negotiated VOIP port, and classifying subsequent VOIP packets are performed in a filtering step by

a fast filtering processor. Additionally, the filtering step further includes applying a filter mask to a header of a packet, extracting unmasked information, comparing the unmasked information to a filtering table and executing predetermined filtering actions based upon the comparison to the filtering table.

Claim 32, from which claim 33 depends, recites a method for switching VOIP packets in a data network. The method includes the steps of receiving a first packet in a network switch, determining if the first packet is a VOIP packet, determining a dynamically negotiated VOIP port for a VOIP session from at least one of the first packet and a second packet received in the network switch, if the first packet is determined to be the VOIP packet. The method also includes the steps of classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters and associating a priority with the subsequent packets to avoid network congestion. The step of determining if the first packet is a VOIP packet further includes the steps of applying a filter mask to the packet header, comparing unmasked information from the header to entries in a filter table to determine a match and determining if a VOIP well known port is contained in the packet header.

As will be discussed below, the cited prior art references of Baum, Curry and Klein fail to disclose or suggest the elements of any of the presently pending claims.

Baum teaches a method for managing security in communication session across a hybrid network. Col. 1, lines 4-12. According to figure 1 of Baum, call setup starts when a user establishes IP layer connectivity with the network. Thereafter, the user launches a

VOIP application and populates a telephone number to be called in a data field. Col. 3, line 40 – Col. 4, line 14. The user initiates the call via the VOIP application, which invokes a directory to obtain the IP address of a destination gateway. The VOIP application invokes the gateway to setup the call, by passing to the gateway, the number to be called, the user account number, and password. The gateway then invokes the authentication database to receive authorization to proceed with the call. If authorization was successful, the gateway establishes the PSTN connection and notifies the client software that the call is proceeding. Col. 4, lines 15 – 63.

Figure 3 of Baum is a detailed illustration of the network with a firewall mechanism. According to figure 3, an IP network is connected to a switched telephone network through gateways. The IP network is connected to the gateways through a firewall mechanism that includes a static firewall router, a hub packet switch and a control processor. The static firewall router acts as a rule based packet filter. The rules are automatically and dynamically set. The security is applied to each port on the fly to provide extremely fast operation. Baum teaches the generation and application of customized filters for each conversation, wherein each filter is unique to a specific conversation and disappears on the termination of the conversation. As a result, a high level of security is obtained. The static firewall router copies the signaling which occurs during setup of a communication path and delivers the two data streams to the packet switch which passes the original stream to the addressed gateway and the copied stream to the control processor. The control processor monitors and analyzes the setup signaling

which follows and derives critical parameters which are used to govern the ensuing conversation. The control processor then compiles a filter code from the parameters and sends the filter code to the firewall. Col. 5, line 24 – Col. 6, line 32.

According to figures 3 and 4 of Baum, the PC initiates the call via the VOIP application and is authenticated and registered through the authorization platform. The directory is accessed to obtain the IP address of the destination gateway. The PC notes the address of the gateway and uses the address to send a Q.931 message to setup a conversation. The message reaches the static firewall which has only one port open for Q.931 messages. If the message is a valid Q.931 stream and includes the Q.931 port address in the firewall and the IP address of the gateway, the firewall commences replication of the signaling stream and passes both streams to the packet switch. The packet switch sends the original stream to the gateway and the copied stream to the control processor. The control processor analyzes the replicated stream and notes that it has a request, where it originated and that it is an H.232 over Q.931 set up signal. The gateway verifies that it has a valid customer and sends a negotiation message, with a proposal of the gateway for a codec and port, back to the PC. The negotiation message passes through the firewall which copies the message and sends the copy to the control processor. The control processor reads and analyzes the replicated message, notes the codec and port and notes that the gateway has authorized the call. An acceptance message is received by the gateway and the gateway returns an acknowledgement to the call via the switch and the firewall. This message is copied by the firewall and sent to the

control processor which registers that a valid conversation as been established on a designated port. The control processor then generates a set of security specifications, compiles a filter configuration message and sends the message to the firewall. The firewall sets up a very specific filter for this single conversation. The firewall now monitors every packet that follows for conformance with the filter requirements. The control processor drops out and turns to other set-ups. Col. 6, line 36 – Col. 9, line 19.

Curry teaches providing telephony communication through a packet switched data network and an organization having a telephone and computer terminals connected to a LAN. To address security issues associated with TCP/IP protocol, Curry relies on a hardware address filter table. The address filter table may be applied to both incoming and outgoing addresses. Col. 5, line 64 - Col. 6, line 28.

Klein teaches that a reliable and simple means of awakening sleeping computers is to maintain a network interface subsystem at full power and to filter detected packets so that when a desired packet is detected, full power is restored to the entire computer. Each of the filters has a 32 bit mask and a 8-bit offset. Klein also teaches that the packet protocol of a VLAN packet is accommodated by reading the VLAN type and incrementing the offset. The VLAN type is expected to be assigned to bytes 12-13 of the VLAN header and bytes 14-15 of the VLAN header are expected to include the VLAN identifier, priority information, and a bit indicating fragmentation in Ethernet packets. Col. 9, lines 1-60.

Applicants respectfully submit that a combination of Baum, Curry and Klein fails to teach or suggest the combination of elements recited in claims 11, 15, 20, 31 and 32. Each of claims 11, 31, and 32, in part, recite determining a dynamically negotiated VOIP port for VOIP session from at least one of the first packet and a second packet received in the switch, if the first packet is the VOIP packet. The Office Action stated that Col. 5, lines 61-67, figure 3, and Col. 7, lines 30-33 of Baum teach this feature of claims 11, 31, and 32. Indeed, Col. 5, lines 61-67 of Baum teaches that rules that are dynamically applied to each port are dynamically and automatically set. If Applicants accept that the dynamic setting of rules applied to each port as taught in Baum, is equivalent to dynamically negotiating VOIP port for VOIP session as recited in claims 11, 31, and 32, Applicants, nevertheless, submit Baum does not teach or suggest determining dynamic setting of rules as applied to each port <u>from at least one of the first packet and a second packet received in the switch, if the first packet is the VOIP packet</u> as recited in claims 11, 31 and 32. As noted above, Col. 7, lines 25-54 of Baum teaches that when the gateway receives the original packet stream from the switch, the gateway checks that the user of the PC is a valid customer and sends <u>a negotiation message,</u> with a proposal of the gateway for a codec and port, back to the PC through the firewall, where the control processor notes the codec, port and the authorization, notes an acceptance message received at the gateway, registers that a valid conversation has been established on a designated port, and sends a filter for the conversation that is to be applied to the port. As such, Baum teaches that the dynamically negotiated port is determined from the gateway

negotiation/authorization message and acceptance message received at the gateway and not from at least one of the first packet and a second packet received in the switch, if the first packet is the VOIP packet as recited in claims 11, 31 and 32.

Claims 11, 15, 31, and 32 also recite, in part, classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters and associating a priority with the subsequent packets to avoid network congestion. Although the Office Action admits that Baum does not teach or suggest associating a priority with the subsequent packets to avoid network congestion, the Office Action states that Col. 7, lines 41-55 of Baum teaches monitoring every packet for conformance to the set of security specifications. The Office Action suggests that monitoring every packet for conformance to the set of security specifications and classifying the packets as belonging to this single conversion, as taught in Baum, is equivalent to the classifying element of claims 11, 15, 31, and 32. Beside the fact that Baum does not teach or suggest any processing of VOIP packets, Applicants submit that the act of monitoring is not the same as act of classifying. Monitoring is defined as the act of checking or supervising while classifying is defined as the act of organizing or arranging according to class or category. (See Webster's II New College Dictionary) Baum teaches monitoring/checking/supervising to ensure that every packet that follows is in conformance with the strict filter requirements. There is simply no discussion or suggestion in Baum of classifying/organizing/arranging all subsequent VOIP packets corresponding to the VOIP port in accordance with the predetermined parameters and

associating a priority with the subsequent packets to avoid network congestion as recited in claims 11, 15, 31, and 32. Furthermore, even if as the Office Action alleges monitoring to ensure that every packet that follows is in conformance with the strict filter requirements, as taught in Baum, is equivalent to classifying all subsequent VOIP packets corresponding to the VOIP port in accordance with the predetermined parameters as recited in claims 11, 15, 31, and 32, there is no teaching or suggestion in Baum of associating a priority with the subsequent packets based on the monitoring step. The Office Action cites Klein as teaching associating a priority with the subsequent packets to avoid network congestion as recited in claims 11, 15, 31, and 32. As noted above, the cited section of Klein merely discloses that priority information is assigned to some bytes in a VLAN header. There is no teaching or suggestion in Klein of processing VOIP packets. Specifically, there is no teaching or suggestion in Klein of classifying all subsequent VOIP packets corresponding to the VOIP port in accordance with the predetermined parameters and associating a priority with the subsequent VOIP packets to avoid network congestion as recited in claims 11, 15, 31, and 32.

Claims 11 and 15 also recite that the classifying step includes a storing step which includes generating a filter corresponding to the dynamically negotiated VOIP port and storing the generated filter in a filter table associated with a fast filter processor. Each of claims 31 and 31 also recites comparing unmasked information from the header to entries in a filter table to determine a match. Claim 20 also recites at least one filtering table in communication with the fast filtering processor. According to the Office Action, Curry

teaches storing the generated filter in a filter table and it would have be obvious to add the filter table associated with a fast filtering processor of Curry to the system of Baum. As noted above, Baum also details that "[e]ach filter is **unique** to a specific conversation. The *filter disappears on termination of the conversation.* As a result a high level of security is obtained." (column 6, lines 2-5, emphasis added). Based on the disclosure, there would be no reason to store any of the filters prepared and thus Baum teaches away from such storage and espouses the benefits of the temporary nature of the filter used. As such, Applicants respectfully assert that given the teachings of Baum, it would not have been obvious to one of ordinary skill in the art "to store this information that the firewall filter uses in a table," as the Office Action urges.

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). Given the clear teachings of Baum, Applicants respectfully assert that independent claims 11, 15, 20, 31 and 32, which all recite, in part, the use of a filter table, are not obvious in view of Baum

Claim 20, in part, recites the fast filtering processor is configured to snoop packets being transmitted through the network switch to trap a VOIP call setup message, and thereafter, determine a dynamically negotiated VOIP port so that all subsequent VOIP packets can be filtered and assigned an appropriate priority. The Office Action suggests that the firewall of Baum is equivalent to the fast filtering processor recited in the

presently pending claims. According to Col. 7, lines 41-55 of Baum the firewall sets up specific filter for each conversation and monitors every packet for conformance with the strict filter requirements. Applicants submit that Baum simply does not teach or suggest that the firewall of Baum is configured to snoop packets being transmitted through the network switch to trap a VOIP call setup message. Baum also does not teach or suggest that the firewall is configured to determine a dynamically negotiated VOIP port so that all subsequent VOIP packets can be filtered and assigned an appropriate priority as recited in claim 20. In fact, as noted above, the Office Action acknowledges that there is no teaching or suggestion in Baum of assigning priority to VOIP packets. Thus, the firewall of Baum is not equivalent to the fast filter processor recited in the pending claims.

Curry and Klein fail to cure any of the deficiencies of Baum. Specifically, Curry and Klein also do not discuss or suggest the fast filtering processor is configured to snoop packets being transmitted through the network switch to trap a VOIP call setup message, and thereafter, determine a dynamically negotiated VOIP port so that all subsequent VOIP packets can be filtered and assigned an appropriate priority as recited in claim 20. Therefore, Applicants respectfully assert that the rejection under 35 U.S.C. §103(a) should be withdrawn because neither Baum, Klein nor Curry, whether taken singly or combined, teaches or suggests each feature of claims 11, 15, 20, 31 and 32 and hence, dependent claims 8, 9, 12-14, 16-19, 27-29 and 33 thereon.

In view of the above, Applicants respectfully submit that independent claims 11, 15, 20, 31 and 32 each recite subject matter which is neither disclosed nor suggested in a

combination of Baum, Curry and Klein. In addition, claims 7-9, 12-14, 16-19, 21-30 and 33, depend from the independent claims and should likewise be allowed for at least their dependence on the independent claims. It is therefore respectfully requested that all of claims 7-9 and 11-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Arlene P. Neal
Registration No.: 43,828

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14^{TH} Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802
APN:kmp